

Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application.

1. - 4. (Canceled)

5. (original) In a wireless network environment comprising at least one authorized access point, a method for containing rogue access points, the rogue access points including a virtual carrier-sense mechanism operative to adjust a counter in response to wireless frames transmitted from wireless stations, wherein the data frames include a duration value, the counter controlling the transmission of frames by the rogue access point, comprising

- detecting a rogue access point,
- identifying at least one authorized access point that neighbors the rogue access point;
- selecting at least one authorized access point in the identifying step;
- configuring the at least one selected access point to periodically transmit wireless frames, the data frames including a predetermined duration value, and wherein the interval at which the data frames are periodically transmitted is less than the duration value.

6. (original) The method of claim 5 wherein the wireless frames are transmitted on all available frequency channels.

7. (original) The method of claim 5 further comprising

- identifying the channel on which the rogue access point is transmitting; and wherein the wireless frames are transmitted on the identified channel.

8. (original) The method of claim 5 further comprising

- identifying the channel on which the rogue access point is transmitting; and wherein the wireless frames are transmitted on a range of channels centered on the identified channel.

9. -14. (canceled)

15. (previously presented) In a wireless network environment implementing a protocol according to which wireless stations terminate connections with access points upon receipt of de-authentication and/or disassociation frames, a method for containing rogue access points, comprising

- detecting a rogue access point, the rogue access point identified by a wireless network address;

- selecting at least one authorized access point;

- emulating the rogue access point and periodically broadcasting, at repetition interval, beacon frames, wherein the beacon frames announce a contention-free period, and wherein the contention-free period is greater than the repetition interval.

16.-23. (canceled)

24. (previously presented) A wireless network system enabling a directed association mechanism, comprising

- a plurality of access elements for wireless communication with at least one remote client element and for communication with a central control element;

- a central control element for supervising at least one of said access elements, wherein the central control element is operative to manage and control the wireless connections between the access elements and corresponding remote client elements; and

- wherein the access elements are each operative to:

- establish and maintain, in an access point mode, wireless connections with remote client elements;

- switch to a scanning mode for a scanning period at a scanning interval to detect wireless traffic,

- record scan data characterizing the detected wireless traffic, and

- transmit the scan data to the central control element;

- wherein the central control element is operative to

- process the scan data against information relating to known access elements to identify rogue access points,

to contain the detected rogue access point(s); and
wherein the central control element is operative to
establish a tunnel with access elements for transmission of wireless traffic
associated with corresponding remote client elements, and
bridge network traffic between a computer network and a remote client
element through a tunnel with a corresponding access element.

25. (canceled)

26. (previously presented) The system of claim 24 wherein the computer network comprises at least one network device operative to switch or route data units between devices connected thereto, the data units including a source address and a destination address, wherein the at least one network device comprises at least two ports to which other devices connect, and wherein the at least one network device is operative to store the source addresses of the data units encountered at the ports of the at least one network device, and

wherein the central control element is operative to
determine the address of at least one rogue client associated with the rogue access
point; and

identify the port to which the rogue access point is connected by querying, using the
addresses of the at least one rogue client, the at least one network device for the port at which data
units sourced from the at least one rogue client were encountered.

27. (original) The system of claim 26 wherein the central control element is operative to report the
identified port to a network administrator.

28. (original) The system of claim 26 wherein the central control element is operative to disable
the identified port.

29. (previously presented) The system of claim 24 wherein the central control element is operative
to configure one or more access elements to contain the detected rogue access point(s).

30. (original) The system of claim 29 wherein the central control element is operative to configure one or more of the access elements to emulate the rogue access point and transmit connection-terminating frames.

31. (original) The system of claim 30 wherein the connection terminating frames are de-authentication frames.

32. (original) The system of claim 30 wherein the connection terminating frames are disassociation frames.

33. (original) The system of claim 30 wherein the connection terminating frames are transmitted at a fixed repetition interval.

34. (original) The system of claim 30 wherein the connection-terminating frames are transmitted as a repetition interval, and wherein the repetition interval is adjusted in response to detection of wireless traffic transmitted between the rogue access point and a wireless client.